July 22, 2008

Non-GSM Mobile Device Tool Specification and Test Plan

Draft 2 for public comment of Version 1.0

National Institute of Standards and Technology
U.S. Department of Commerce

Abstract

As mobile devices proliferate, incorporating a host of integrated features and capabilities, their use can be seen everywhere in our world today. Mobile communication devices contain a wealth of sensitive and non-sensitive information. In the investigative community their use is not restricted to data recovery alone as in criminal cases, but also civil disputes and proceedings, and their aggregate use in research and criminal incident recreation continues to increase. Due to the exploding rate of growth in the production of new mobile devices appearing on the market each year is reason alone to pay attention to test measurement means and methods. The methods a tool uses to capture, process, and report data must incorporate a broad range of extensive capabilities to meet the demand as a robust data acquisition tool. In general, a forensic examination conducted on a mobile device is only a small subset of the larger field of digital forensics. Consequentially, tools possessing an exhaustive array of capabilities to acquire data from these portable mobile devices are relatively few in number.

This paper defines requirements for mobile device applications capable of acquiring data from mobile devices operating over a Code Division Multiple Access (CDMA) network, test methods used to determine whether a specific tool meets the requirements, and assertions derived from requirements producing measurable results.[•] The test assertions are described as general statements of conditions that can be checked after a test is executed. Each assertion appears in one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

Your comments and feedback are welcome; revisions of this document are available for download at: http://www.cftt.nist.gov/mobile_devices.htm.

[•] NIST does not endorse nor recommend products or trade names identified in this paper. All products used in this paper are mentioned for use in research and testing by NIST.

TABLE OF CONTENTS

1. Introduction

The need to ensure the reliability of mobile device forensic tools intensifies, as the embedded intelligence and ever-increasing storage capabilities of mobile devices expand. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools. This is accomplished by the development of both specific and common rules that govern tool specifications. We adhere to a disciplined testing procedure, established test criteria, test sets, and test hardware requirements, that result in providing necessary feedback information to toolmakers so they can improve their tool's effectiveness; end users benefit in that they gain vital information making them more informed about choices for acquiring and using computer forensic tools, and lastly, we impart knowledge to interested parties by increasing their understanding of a specific tool's capability. Our approach for testing computer forensic tools is based on established well-recognized international methodologies for conformance testing and quality testing. For more information on mobile device forensic methodology please visit us at: http://www.cftt.nist.gov/.

The Computer Forensic Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the research and development organization of the U.S. Department of Justice, and the National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and the U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

The central requirement for a sound forensic examination of digital evidence is that the original evidence must not be modified (i.e., the examination or capture of digital data from a mobile device and associated media must be performed without altering the device or media content). In the event that data acquisition is not possible using current technology to access information without configuration changes to the device (e.g., loading a driver), the procedure must be documented and minimal (i.e., file size) to accomplish the required task.

2. Purpose

This document defines requirements for mobile device forensic tools used in digital forensics capable of acquiring internal memory from Code Division Multiple Access (CDMA) devices and test methods used to determine whether a specific tool meets the requirements.

The requirements that will be tested are used to derive assertions. The assertions are described as general statements of conditions that can be checked after a test is executed. Each assertion generates one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

3. Scope

The scope of this specification is limited to software tools capable of acquiring CDMA devices. The specifications are general and capable of being adapted to other types of mobile device software tailored for GSM devices.

4. Test Assertions

The primary goal of test assertions A_IM-01 – A_IMO-40, presented below in Table 1, is to determine the tools ability to acquire specific data elements pre-populated onto the device without modification. The ID column identifies the medium (i.e., mobile device internal memory) the test is being performed on. For instance A_IM-01 is an assertion performed on the internal memory (IM) of a mobile device. Assertions A_IMO-# (internal memory optional) is an optional assertion and only tested if a tool supports the feature. If the tool does not provide the capability defined, the test assertion does not apply. The Test Assertion column states the assertion and the comments column provides additional information pertaining to the assertion.

Table 1: Test Assertions

ID	Test Assertion	Comments
A_IM-01	If a cellular forensic tool provides support for connectivity of the target device then the tool shall successfully recognize the target device via all vendor supported interfaces (e.g., cable, Bluetooth, IrDA).	Connect supported device via supported interface(s); Begin acquisition to determine if successful
A_IM-02	If a cellular forensic tool attempts to connect to a non-supported device then the tool shall have the ability to identify that the device is not supported.	Connect a non-supported device; Begin acquisition to determine if the application provides a message that the device is not supported
A_IM-03	If a cellular forensic tool encounters disengagement between the device and application then the application shall notify the user that connectivity has been disrupted.	Begin acquisition; Disconnect interface or interrupt connectivity (i.e., unplug cable) during acquisition to determine if the tool provides an error message
A_IM-04	If a cellular forensic tool successfully completes acquisition of the target device then the tool shall have the ability to present	Examine acquired data via supported report (e.g., preview-pane view,

	acquired data elements in a human-readable format via either a preview-pane view or a generated report.	generated report) for readability
A_IM-05	If a cellular forensic tool successfully completes acquisition of the target device then subscriber related information shall be presented in a human-readable format without modification.	MSISDN is reported
A_IM-06	If a cellular forensic tool successfully completes acquisition of the target device then equipment related information shall be presented in a human-readable format without modification.	MEID/ESN is reported
A_IM-07	If a cellular forensic tool successfully completes acquisition of the target device then all known address book entries shall be presented in a human-readable format without modification.	Address book entries and associated data (i.e., phone number) are reported.
A_IM-08	If a cellular forensic tool successfully completes acquisition of the target device then all known maximum length address book entries shall be presented in a human-readable format without modification.	Maximum length address book entries (i.e., contact name) are reported in totality
A_IM-09	If a cellular forensic tool successfully completes acquisition of the target device then all known address book entries containing special characters shall be presented in a human-readable format without modification.	Address book entries containing special characters (e.g., #, !, *) are reported
A_IM-10	If a cellular forensic tool successfully completes acquisition of the target device then all known address book entries containing blank names shall be presented in a human-readable format without modification.	Address book entries containing blank names are reported
A_IM-11	If a cellular forensic tool successfully completes acquisition of the target device then all known email addresses associated with address book entries shall be presented in a human-readable format without modification.	Address book entries containing an email addresses are reported

A_IM-12	If a cellular forensic tool successfully completes acquisition of the target device then all known graphics associated with address book entries shall be presented in a human-readable format without modification.	Address book entries containing an graphic are reported
A_IM-13	If a cellular forensic tool successfully completes acquisition of the target device then all known datebook, calendar, and note entries shall be presented in a human-readable format without modification.	Datebook/calendar, notes entries are reported
A_IM-14	If a cellular forensic tool successfully completes acquisition of the target device then all maximum length datebook, calendar, and note entries shall be presented in a human-readable format without modification.	Maximum length datebook/calendar, notes entries are reported
A_IM-15	If a cellular forensic tool successfully completes acquisition of the target device then all call logs (incoming/outgoing) shall be presented in a human-readable format without modification.	Incoming and outgoing calls are reported
A_IM-16	If a cellular forensic tool successfully completes acquisition of the target device then all text messages (i.e., SMS, EMS) messages shall be presented in a human-readable format without modification.	Text messages stored in the internal memory are reported
A_IM-17	If a cellular forensic tool successfully completes acquisition of the target device then all MMS messages and associated audio shall be presented properly without modification.	Incoming and outgoing MMS message data including text and audio are reported
A_IM-18	If a cellular forensic tool successfully completes acquisition of the target device then all MMS messages and associated images shall be presented properly without modification.	Incoming and outgoing MMS message data including text and graphical images are reported
A_IM-19	If a cellular forensic tool successfully completes acquisition of the target device then all MMS messages and associated video shall be presented properly without modification.	Incoming and outgoing MMS message data including text and video are reported

A_IM-20	If a cellular forensic tool successfully completes acquisition of the target device then all stand-alone audio files shall be acquired and playable via either an internal application or suggested third-party application without modification.	Stand-alone audio files are reported
A_IM-21	If a cellular forensic tool successfully completes acquisition of the target device then all stand-alone image files shall be viewable via either an internal application or suggested third-party application without modification.	Stand-alone graphic files (i.e., images) are reported
A_IM-22	If a cellular forensic tool successfully completes acquisition of the target device then all stand-alone video files shall be viewable via either an internal application or suggested third-party application without modification.	Stand-alone video files are reported
A_IMO-23	If a cellular forensic tool successfully completes acquisition of the target device then the tool shall present the acquired data without modification via supported generated report formats.	Check report output with known data elements for consistency and completeness
A_IMO-24	If a cellular forensic tool successfully completes acquisition of the target device then the tool shall present the acquired data without modification in a preview-pane view.	Check preview-pane output with known data elements for consistency and completeness
A_IMO-25	If a cellular forensic tool provides a preview-pane view and a generated report of the acquired data then the reports shall maintain consistency of all reported data elements.	Check generated report and preview-pane for consistency if both supported
A_IMO-26	If modification is attempted to the case file or individual data elements via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification.	Data integrity
A_IMO-27	If the cellular forensic tool supports a physical acquisition of the target device then the tool shall successfully complete the acquisition and present the data in a human-readable format.	Physical acquisition; Readability of acquired data

A_IMO-28	If the cellular forensic tool supports a physical acquisition of address book entries present on the target device then the tool shall report recoverable deleted entries or data remnants in a human-readable format	Physical acquisition; Recovery of deleted address book entries
A_IMO-29	If the cellular forensic tool supports a physical acquisition of calendar, tasks, or notes present on the target device then the tool shall report recoverable deleted calendar, tasks, or note entries or data remnants in a human-readable format.	Physical acquisition; Recovery of deleted calendar, tasks, note entries
A_IMO-30	If the cellular forensic tool supports a physical acquisition of call logs present on the target device then the tool shall report recoverable deleted call log data or data remnants in a human-readable format.	Physical acquisition; Recovery of deleted call logs
A_IMO-31	If the cellular forensic tool supports a physical acquisition of SMS messages present on the target device then the tool shall report recoverable deleted SMS messages or SMS message data remnants in a human-readable format.	Physical acquisition; Recovery of deleted SMS messages
A_IMO-32	If the cellular forensic tool supports a physical acquisition of EMS messages present on the target device then the tool shall report recoverable deleted EMS messages or EMS message data remnants in a human-readable format.	Physical acquisition; Recovery of deleted EMS messages
A_IMO-33	If the cellular forensic tool supports a physical acquisition of audio files present on the target device then the tool shall report recoverable deleted audio data or audio file data remnants in a human-readable format.	Physical acquisition; Recovery of deleted audio files
A_IMO-34	If the cellular forensic tool supports a physical acquisition of graphic files present on the target device then the tool shall report recoverable deleted graphic file data or graphic file data remnants in a human-readable format.	Physical acquisition; Recovery of deleted image files
A_IMO-35	If the cellular forensic tool supports a physical acquisition of video files present on the target device then the tool shall report	Physical acquisition; Recovery of deleted video files

	recoverable deleted video file data or video file data remnants in a human-readable format.	
A_IMO-36	If the cellular forensic tool supports log creation then the application should present the log files consistent with the application documentation (e.g., outlining the acquisition process).	Log file creation
A_IMO-37	If the cellular forensic tool supports proper display of foreign language character sets then the application should present address book entries containing foreign language characters in their native format without modification.	Acquisition and display of foreign language character sets
A_IMO-38	If the cellular forensic tool supports proper display of foreign language character sets then the application should present text messages containing foreign language characters in their native format without modification.	Acquisition and display of foreign language character sets
A_IMO-39	If the cellular forensic tool supports hashing for individual data objects then the tool shall present the user with a hash value for each supported data object.	Individual data object hash reporting
A_IMO-40	If the cellular forensic tool supports hashing the overall case file then the tool shall present the user with one hash value representing the entire case data.	Case file hash reporting

5. Abstract Test Cases

Abstract test cases describe the combinations of test parameters required to fully test each assertion and the results expected for the given combination of test parameters. The test cases are abstract in that they do not prescribe the exact environment in which the tests are to be performed. They are written at the next level above the environment. This allows different environments to be substituted under the test cases for testing different products and options.

5.1 Test Cases for Core Features.

<u>Mobile Device Internal Memory Test Cases</u>:

CFT-IM-01 Acquire mobile device internal memory over supported interfaces (e.g., cable, Bluetooth, IrDA).

CFT-IM-02 Attempt internal memory acquisition of a non-supported mobile device.

CFT-IM-03 Begin mobile device internal memory acquisition and interrupt connectivity by interface disengagement.

CFT-IM-04 Acquire mobile device internal memory and review reported data via the preview-pane or generated reports for readability.

CFT-IM-05 Acquire mobile device internal memory and review reported subscriber and equipment related information (i.e., MEID/ESN, MSISDN).

CFT-IM-06 Acquire mobile device internal memory and review reported PIM related data.

CFT-IM-07 Acquire mobile device internal memory and review reported call logs.

CFT-IM-08 Acquire mobile device internal memory and review reported text messages.

CFT-IM-09 Acquire mobile device internal memory and review reported MMS multi-media related data (i.e., text, audio, graphics, video).

CFT-IM-10 Acquire mobile device internal memory and review reported stand-alone multi-media data (i.e., audio, graphics, video).

5.2 Test Cases for Optional Features

The following requirements are defined for tool features that might be implemented for some cellular forensic tools. If a tool provides the optional feature, the tool is tested as if the requirement were mandatory. If the tool does not provide the capability defined, the requirement does not apply.

<u>Optional Internal Memory Assertions</u>:

CFT-IMO-01 Acquire mobile device internal memory and review reported data via supported generated report formats.

CFT-IMO-02 Acquire mobile device internal memory and review reported data via the preview-pane.

CFT-IMO-03 Acquire mobile device internal memory and compare reported data via the preview-pane and supported generated reports.

CFT-IMO-04 After a successful mobile device internal memory acquisition, alter the case file via third-party means and attempt to re-open the case file.

CFT-IMO-05 Perform a physical acquisition and review data output for readability.

CFT-IMO-06 Perform a physical acquisition and review reports for recoverable deleted data.

CFT-IMO-07 Acquire mobile device internal memory and review generated log files.

CFT-IMO-08 Acquire mobile device internal memory and review data containing foreign language characters.

CFT-IMO-09 Acquire mobile device internal memory and review hash values for vendor supported data objects.

CFT-IMO-10 Acquire mobile device internal memory and review the overall case file hash.

Each test assertion specifies a set of conditions that can be tested and the expected results. A traceability matrix relating requirements and assertions is illustrated below.

Requirements to Test Cases (Device Memory - Core Features)

Test Cases											
Device Memory Requirements (Core Features)		**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**
	CFT-IM-01	•									
	CFT-IM-02		•								
	CFT-IM-03	•		•							
	CFT-IM-04	•			•						
	CFT-IM-05	•			•	•	•	•	•	•	•

Requirements to Test Cases (Device Memory – Optional Features)

		Test Cases									
		01	02	03	04	05	06	07	08	09	10
Device Memory Requirements (Optional Features)	CFT-IMO-01	•		•							
	CFT-IMO-02		•	•							
	CFT-IMO-03				•						
	CFT-IMO-04	•	•			•	•				
	CFT-IMO-05							•			
	CFT-IMO-06	•	•						•		
	CFT-IMO-07	•	•							•	
	CFT-IMO-08	•	•								•

Test Cases to Assertions (Device Memory – Core Features) – Part 1

Test Assertions													
		01	02	03	04	05	06	07	08	09	10	11	12
Device Memory Test Cases (Core Features)	CFT-IM-01	•											
	CFT-IM-02		•										
	CFT-IM-03	•		•									
	CFT-IM-04	•			•								
	CFT-IM-05	•			•	•	•						
	CFT-IM-06	•			•			•	•	•	•	•	•
	CFT-IM-07	•			•								
	CFT-IM-08	•			•								
	CFT-IM-09	•			•								
	CFT-IM-10	•			•								

Test Cases to Assertions (Device Memory – Core Features) – Part 2

		Test Assertions									
		13	14	15	16	17	18	19	20	21	22
Device Memory Test Cases (Core Features)	CFT-IM-01										
	CFT-IM-02										
	CFT-IM-03										
	CFT-IM-04										
	CFT-IM-05										
	CFT-IM-06	•	•								
	CFT-IM-07			•							
	CFT-IM-08				•						
	CFT-IM-09					•	•	•			
	CFT-IM-10								•	•	•

Test Cases to Assertions (Device Memory – Optional Features) – Part 1

Test Assertions													
Device Memory Test Cases (Optional Features)		23	24	25	26	27	28	29	30	31	32	33	34
	CFT-IMO-01	•											
	CFT-IMO-02		•										
	CFT-IMO-03	•	•	•									
	CFT-IMO-04				•								
	CFT-IMO-05	•	•			•							
	CFT-IMO-06	•	•				•	•	•	•	•	•	•
	CFT-IMO-07												
	CFT-IMO-08	•	•										
	CFT-IMO-09	•	•										
	CFT-IMO-10	•	•										

Test Cases to Assertions (Device Memory – Optional Features) – Part 2

		Test Cases					
Device Memory Test Cases (Optional Features)		**35**	**36**	**37**	**38**	**39**	**40**
	CFT-IMO-01						
	CFT-IMO-02						
	CFT-IMO-03						
	CFT-IMO-04						
	CFT-IMO-05						
	CFT-IMO-06	•					
	CFT-IMO-07		•				
	CFT-IMO-08			•	•		
	CFT-IMO-09					•	
	CFT-IMO-10						•